PURPOSE

To establish safeguards that must be implemented by the Michigan Department of Health and Human Services (MDHHS) workforce to protect the confidentiality of sensitive or protected health information (PHI), personally identifiable information (PII), sensitive or confidential information while stored, in use, or disclosed as permitted under all applicable confidentiality laws.

REVISION HISTORY

Reviewed:01/01/2022.
Next Review: 01/01/2023.

POLICY

MDHHS workforce shall use appropriate administrative, technical, and physical safeguards to protect the confidentiality, availability, integrity, privacy, and security of PHI, PII, sensitive or confidential information. MDHHS workforce will only use or disclose PHI, PII, sensitive or confidential information as permitted under all applicable confidentiality laws. MDHHS workforce must use PHI, PII, sensitive or confidential information only to perform work duties. MDHHS workforce members will follow the department's policy and procedures for the use or disclosure of the minimum necessary and for verification of the recipient's authority to receive PHI, PII, sensitive or confidential information. MDHHS workforce members should also assess whether a limited data set may be disclosed upon execution of a data use agreement.

A HIPAA covered component within MDHHS will not disclose PHI, PII, sensitive or confidential information to a non-covered component within the department unless the purpose for the disclosure is permitted in the rules and other applicable confidentiality law, or a signed HIPAA compliant authorization has been obtained from the individual.

PROCEDURE

When sharing, transporting, transmitting, or otherwise preparing PHI, PII, sensitive or confidential information for transmission/transporting outside of work area, the MDHHS workforce will consider all formats and use the most secure method under the circumstances; including, where applicable, appropriate encryption standards. MDHHS workforce will also use or disclose only the minimum amount of PHI, PII, sensitive or confidential information necessary to accomplish the intended purpose and will

consider whether codes can be used an alternative to direct identifiers.

Set forth below are procedures establishing minimum administrative, technical, and physical standards that the MDHHS workforce must follow to protect the confidentiality, availability, and integrity of PHI, PII, sensitive or confidential information. Department components may develop additional policies and procedures that are stricter than the parameters set forth below in order to maximize the protection of PHI, PII, sensitive or confidential information in light of the unique circumstances of a particular area.

A process (ongoing or one-time) that deviates from this policy and procedure must be documented by the business area and approved by the MDHHS Compliance and Data Governance Bureaur prior to implementation.

Verbal Communications

MDHHS workforce members will not discuss PHI, PII, sensitive or confidential information outside of work areas or without a business need within work areas.

Only the minimum necessary PHI, PII, sensitive or confidential information should be disclosed during oral conversations when necessary to further treatment, payment, or health care operations, or for other permitted purposes.

Fax

- Machines and programs capable of sending and receiving faxes must be located in secure areas not readily accessible by visitors.

- Fax only the minimum necessary to accomplish the permitted and intended purpose. The faxing of Federal Tax Information (FTI) is not permitted.

  When faxing, verify fax number by viewing the phone number on the fax machine before pushing the send button. Include a cover sheet with the following confidentiality disclaimer: Confidentiality Notice: The information contained in this facsimile message from the Michigan Department of Health and Human Services is intended solely for the use of the above named recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use,

disclosure, or distribution of any confidential and/or privileged information contained in this fax is expressly prohibited. If you have received this fax in error, please telephone us immediately so that we can correct the error and arrange for destruction or return of the faxed document.

- Incoming faxes containing PHI, PII, sensitive or confidential information should not be left in unsecure areas.

- Confirmation documentation should be reviewed to ensure the intended recipient(s) received the fax. Recipients can be contacted to verify receipt of the fax. The documentation should be maintained with the document that was faxed; see APL 68E-340 for the retention policy.

- Misdirected faxes containing PHI, PII, sensitive or confidential information must be immediately reported; see Misdirected Communications/Transmissions or Breaches That Contain PHI, PII, Sensitive or Confidential Information section in this item.

Scanned Documents

MDHHS workforce members must delete scanned documents immediately after retrieving the documents from the online site or server.

If the device supports it, MDHHS workforce members must password-protect the scanned document. MDHHS workforce members should contact their DTMB liaison for assistance. MDHHS workforce members may also contact MDHHSPrivacySecurity@michigan.gov for assistance.

Email

1. Email of PHI, PII, sensitive or confidential information outside of the State of Michigan (SOM) firewall requires workforce members to comply with the following:

   If appropriate, first consider faxing or phoning PHI, PII, sensitive or confidential information; or use an alternative electronic communication transmission such as the Single Sign-On File Transfer system or other approved secure file exchange method (for example, File Transfer Protocol (FTP), File Transfer Service (FTS)). Contact MDHHSPrivacySecurity@michigan.gov for other possible electronic communication alternatives.

When emailing communications that reference PHI, PII, sensitive or confidential information, always:

- Disclose the minimum amount of PHI, PII, sensitive or confidential information necessary to accomplish the intended purpose of the use, disclosure, or request. The emailing of Federal Tax Information (FTI) is not permitted.
- Ensure that all persons receiving the email have a right to receive the information. The *to* line must be checked to make sure you have the correct email address of the intended recipient before sending the email.
- Include the following disclaimer:

  Confidentiality Notice: This message, including any attachments, is intended solely for the use of the named recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure, or distribution of any confidential and/or privileged information contained in this email is expressly prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy any and all copies of the original message.

Misdirected emails containing PHI, PII, sensitive or confidential information must be immediately reported; see Misdirected Communications/Transmissions or Breaches That Contain PHI, PII, Sensitive or Confidential Information section in this item.

2. Email PHI, PII, sensitive or confidential information within the SOM firewall.

   Email messages sent to addresses that end in Michigan.gov remain within the SOM firewall. All other email messages must be sent using the guidelines in section 3.

   Email exchanges that remain within the SOM firewall must be sent using, at minimum, the guidelines below:

   - Do not include PHI, PII, sensitive or confidential information in the subject line.
   - Use minimal identifiers of PHI, PII, sensitive or confidential information in the body of the email.

- When appropriate, the guidelines in section 3 may be used.

3. Guidelines for all emails outside the SOM firewall containing PHI, PII, sensitive or confidential information:

   When using any of the options below, do not include identifiers or PHI, PII, sensitive or confidential information in the subject line or the body of the email.

   - Option 1: Email information without identifiers in combination with a fax or phone call with the identifiers.

     Example:

     Email: "Beneficiary has called the Beneficiary Help Line and claims that coverage for Ultram has been denied; however, the beneficiary cannot tolerate other pain medications. Please see Fax for identifying information."

     Fax (or phone call): "Email sent at 1:50 pm with KK in the subject line is for Jane Doe, Medicaid ID# 99999999."

   - Option 2: Encrypt and password-protect a document that contains all of the PHI, PII, sensitive or confidential information and attach to the outbound email. Phone or fax the password separately.

4. Receiving unencrypted email with PHI, PII, sensitive or confidential information from outside the SOM firewall.

   Advise the sender that sending information through an unencrypted electronic mail is not secure. When replying, send a separate email following the stated guidelines or remove all identifying information from the original email. If needed, contact MDHHSPrivacySecurity@michigan.gov for other electronic options to exchange PHI, PII, sensitive or confidential information.

Text Messaging

The texting of sensitive or confidential information is not permitted. Texting includes, but is not limited to, Short Message Service (SMS), multimedia messages (MMS), and ideograms.

Other Electronic Communications

Authorized communications transmitted by other electronic systems such as File Transfer Protocol (FTP) or File Transfer Service (FTS) must:

- Be accessed only by the intended recipient(s).
- Contain only the minimum necessary information for the intended purpose of the disclosure.

Paper

All paper with PHI , PII, sensitive or confidential information must be protected from the view of others who do not have a need to know the information to perform their job. Only those individuals that have the business need to access the PHI, PII, sensitive or confidential information are permitted to view the letter, report, form, document, etc. Paper with PHI, PII, sensitive or confidential information may be redacted to remove PHI, PII, sensitive or confidential information. See policy APL 68D-030 and procedure APL 68D-032 for assistance with de-identifying PHI, PII, sensitive or confidential information.

Paper with PHI, PII, sensitive or confidential information that is not presently in use must be turned upside down, placed in a drawer, locked in a file cabinet, or secured in another manner - based on the authorized user's reasonable judgment and present need.

Mail (USPS, certified USPS, or other mail delivery service such as FedEx)

MDHHS workforce must ensure that:

- The last known correct address is used for the intended recipient.
- The complete address information, including apartment numbers when applicable, is used for the intended recipient.
- The address is typed or written in a legible manner.
- The return address appears on the envelope/package.
- The return address does not readily identify a specific MDHHS program.

- The mail envelope or package is appropriate in size, shape and strength for the items being mailed.
- The mail envelope or package is securely sealed.
- Materials placed into the envelope or mail package is only information that is intended for the addressee. Do not send PHI, PII, sensitive or confidential information to an individual who is not authorized to view the PHI, PII, sensitive or confidential information.

Misdirected mail containing PHI, PII, sensitive or confidential information must be immediately reported; see Misdirected Communications/Transmissions or Breaches That Contain PHI, PII, Sensitive or Confidential Information section in this item.

Interoffice Mail

MDHHS workforce must ensure that:

- The correct address is used for the intended recipient.
- The complete location information for the intended recipient is used. Include:
  - Full name.
  - Department.
  - Division.
  - Building.
  - Floor (if applicable and available).
- The address is typed or written in a legible manner.
- The interoffice mail envelope is securely sealed.
- Materials placed in an interoffice envelope or mail package is only information that is intended for the addressee. Do not send PHI, PII, sensitive or confidential information to an individual who is not authorized to view PHI, PII, sensitive or confidential information.

Misdirected interoffice mail containing PHI, PII, sensitive or confidential information must be immediately reported; see Misdirected Communications/Transmissions or Breaches That Contain PHI, PII, Sensitive or Confidential Information section in this item.

Computer Visibility and Access

PHI, PII, sensitive or confidential information on computer screens will not be viewable by a casual observer.

MDHHS workforce members will use a screen saver or position the computer to minimize others' view of the screen.

Computer log-ins will be changed routinely and not shared with others; see APL 68E-100 Password Management Policy and Procedure.

MDHHS workforce members will log-off or lock computer if away from workstation.

Phone Conversations

MDHHS workforce members will ensure that correct telephone numbers are dialed and that the minimum amount of information is used to convey any messages left via telephone or voice mail. PHI , PII, sensitive or confidential information cannot be left on voice mail messages.

Portable Electronic Devices

The use of portable electronic storage devices is not permitted, unless appropriate approval is obtained via the DHHS-5440 form.

Portable electronic devices can include laptop computers, compact discs, thumb or flash drives, iPads, iPhones, Blackberry Phones, or any other portable device that is capable of receiving and storing data from an apparatus that maintains electronic information. The portable electronic device must be DTMB approved and ordered through the appropriate procurement process. Devices must be encrypted using methods meeting SOM standards as required by DTMB 1340.00.07 Electronic Data Encryption Standard. Portable electronic devices must be secured as described in the Securing Portable Electronic Devices section below.

Contact MDHHSPrivacySecurity@michigan.gov for guidance on ordering the appropriate portable electronic device and for assistance with encrypting and password-protecting the device.

Any loss, theft, or breach of PHI, PII, sensitive or confidential information from a portable electronic device must be immediately reporting. See Misdirected Communications/Transmissions or

Breaches That Contain PHI, PII, Sensitive or Confidential Information section below.

Securing Portable Electronic Storage Devices

For all Portable Electronic Storage Devices:

- Only transport the device when required to complete job duties, after receiving approval via the DHHS-5440 form.
- Never leave your device unsecured while unattended.
- Never leave the device in plain view in a vehicle.
- Password-protect the device.

Laptop Computers:

- Make sure an encryption program is installed. Contact MDHHSPrivacySecurity@michigan.gov for guidance on ensuring encryption is installed.
- Secure laptops to workstations using a combination lock or by locking it in a drawer while you are away. Contact MDHHSPrivacySecurity@michigan.gov for information on obtaining and properly installing laptop locks.
- All PHI, PII, sensitive or confidential information must be stored on the designated network drive (not the device's hard drive), as assigned by management.

Flash (thumb) drives or compact discs:

- Any information stored on the device must be encrypted to meet SOM standards.
- Only store or transport information using a DTMB approved device.
- Store the device in a secured location such as a locked drawer at your workstation.

Mobile Devices (iPhones, iPads, Blackberry Phones, Android Phones, etc.)

- Mobile Device Management (MDM) software (for example, MaaS 360) must be installed on the device. Contact

MDHHSPrivacySecurity@michigan.gov for guidance on ensuring MDM is installed on the device.

Destruction: Paper, CDs, Floppies, and other portable media

Paper with PHI, PII, sensitive or confidential information must be shredded or pulverized before recycling. Laptop computers, CDs, floppies, flash drives, or other portable devices must be destroyed prior to disposal.

See policy APL 68E-280 regarding secure disposal procedures. Contact MDHHSPrivacySecurity@michigan.gov for questions about how to have a portable device destroyed.

Misdirected Communications/Transmissions or Breaches that Contain PHI, PII, Sensitive or Confidential Information

All instances of misdirected, unpermitted or unauthorized communications, or breaches that contain PHI, PII, sensitive or confidential information must be reported immediately; see APL 68E-130 for guidelines on how to report.

A breach includes but is not limited to the loss or theft of any paper or electronic devices that contain sensitive or protected health information.

If a mobile device is lost or stolen:

- Immediately call the DTMB Client Service Center (CSC) at 517-241-9700 or 1-800-968-2644, including after hours or on the weekend.
- Request a high priority ticket to be opened with the wireless team.
- Request that the mobile device be remotely wiped.
- Ask the client services representative to reset SOM passwords.

Exceptions

A process (ongoing or one-time) that deviates from this policy and procedure must be documented by the business area and approved by the MDHHS privacy and security officers prior to implementation.

REFERENCES/FORM

45 CFR §164.304, §164.308, §164.310, §164.312, §164.502(a)(1)(iii), §164.502(b}, §164.514(d)(1}, §164.530(c).

DTMB 1340.00.110.03

CONTACT

For additional information concerning this procedure, contact the MDHHS Compliance and Data Governance Bureau at emailMDHHSPrivacySecurity@michigan.gov.